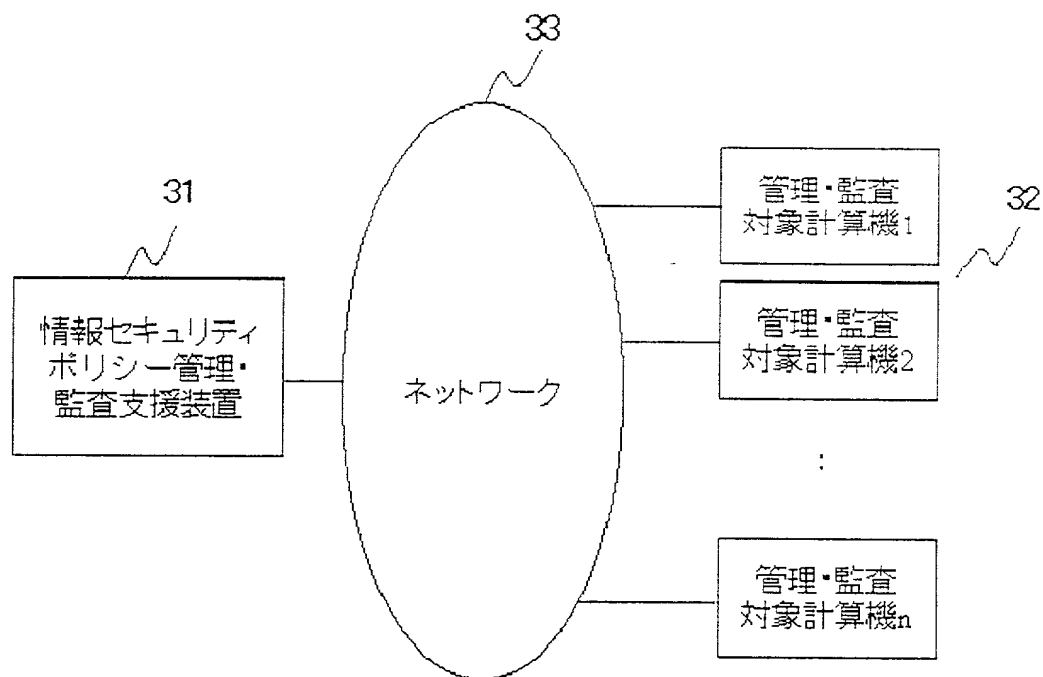


【書類名】図面

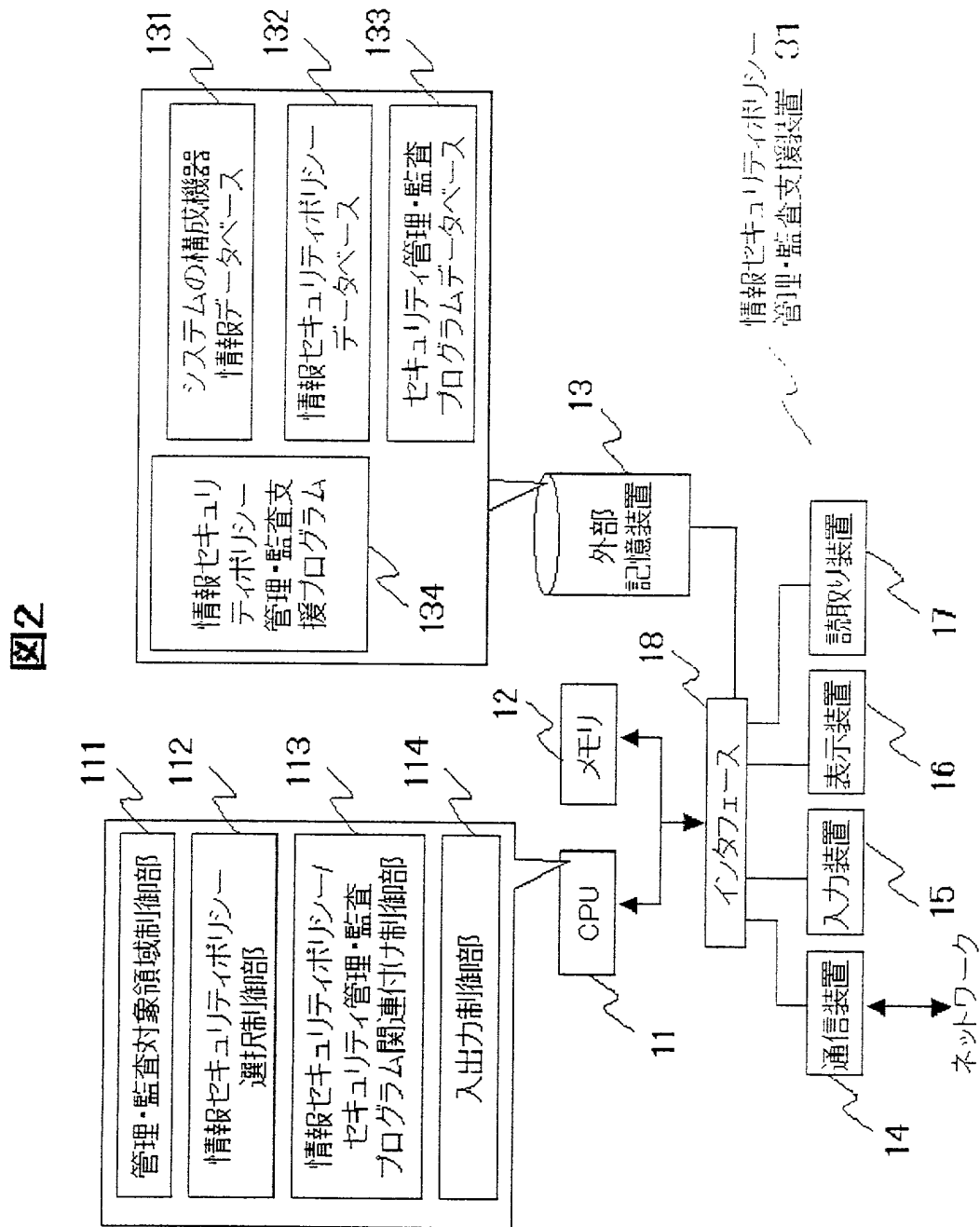
【図1】

図1

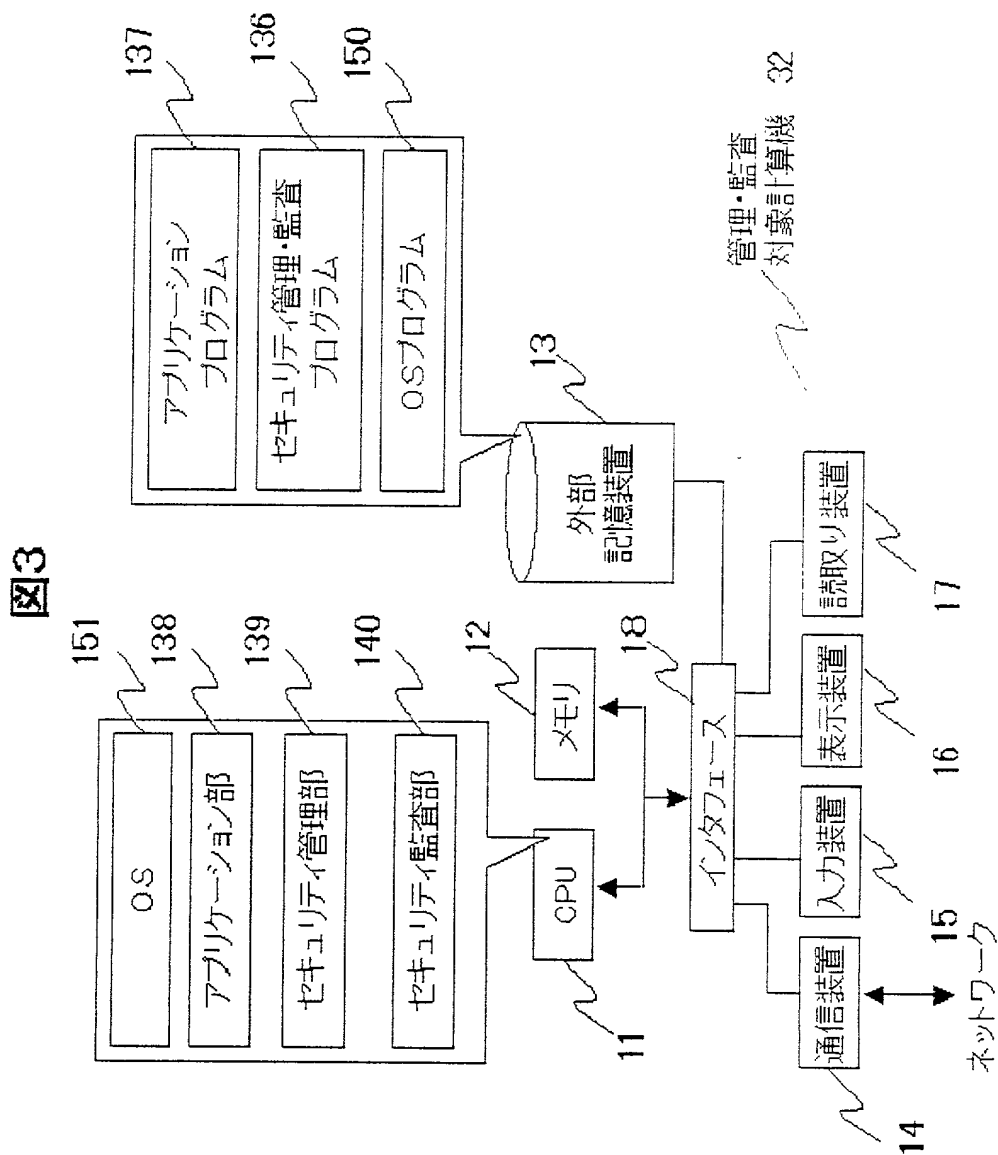


20040406

【図2】



【図3】



【図4】

図4

41 SYSID	42 装置種別	43 ソフトウェア種別	44 プログラム名	45 選択可否
R001-00-01	ルータ	—	A	YES
R001-00-02			B	NO
⋮	⋮	⋮	⋮	⋮
S001-OS-01	サーバ	OS	H	YES
S001-OS-02			I	NO
S001-WEB-01		Web	X	YES
S001-WEB-02			Y	NO
S001-WEB-03			Z	NO
S001-MAIL-01		メール	O	YES
S001-DB-01		データベース	P	YES
⋮	⋮	⋮	⋮	⋮

【図5】

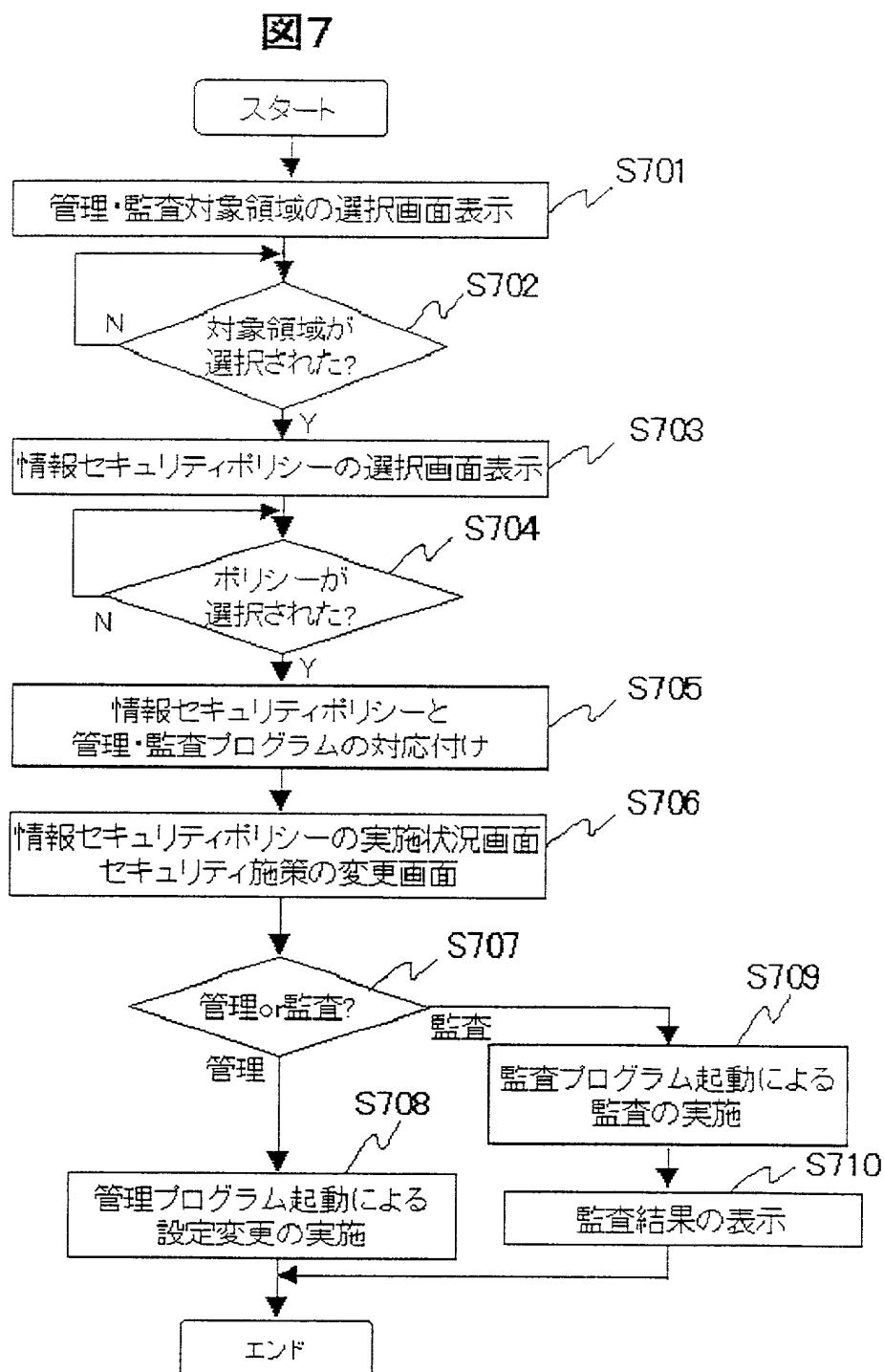
図5

51	52	53	54
POLICYID	施策種別	セキュリティ施策	選択可否
AUTH-01	識別と認証機能	ネットワークにアクセス可能な端末の限定	YES
AUTH-02	識別と認証機能	識別・認証情報用の良いパスワード設定の実施	YES
:	:	:	:
:	:	:	:
ACC-01	アクセス制御機能	端末やユーザ毎に利用可能なコマンドの限定	YES
ACC-02	アクセス制御機能	権限の設定・変更・削除可能者の限定	YES
ACCADM-01	アクセス監視	データ・プログラムの改ざん検出の実施	YES
ACCADM-02	アクセス監視	ユーザ使用コマンドの記録	NO
ACCADM-03	アクセス監視	アクセスログの取得	NO
VIRUS-01	ウィルス対策	ワクデジソフトウェアのインストール	
VIRUS-02	ウィルス対策	定期的なウィルスチェック	YES
VIRUS-03	ウィルス対策	定期的なウィルス定義データの更新	YES
:	:	:	:
:	:	:	:



POLICYID	管理プログラム			監査プログラム		
	管理プログラム名 ADMD	SYSID	対応付け	監査プログラム名 AUDITID	SYSID	対応付け
AUTH-01	ADM[USR_#1	R001-00-01 S001-WEB-01 :	○	AUDIT_USR_#1	S001-WEB-01	○
AUTH-02	ADM[USR_#2	S001-MAIL-01	-	AUDIT_USR_#2	R001-00-01	-
:	:	:	:	:	:	:
:	:	:	:	:	:	:
ACCADM-01	ADM[UNAUTH_#1	S001-MAIL-01	○	AUDIT_LOG_#1	S001-MAIL-01	○
:	:	:	:	:	:	:
:	:	:	:	:	:	:

【図7】



【図8】

図8

情報セキュリティポリシー管理・監査対象領域の選択画面

装置種別	<div>サーバ ▼</div> <div>ルータ サーバ クライアント :</div>	91
ソフトウェア種別	<div>Web ▼</div> <div>OS Web メール :</div>	92
プログラム名	<div>X ▼</div>	93
使用可否	<div>NO ▼</div> <div>YES</div>	94

OK 閉じる

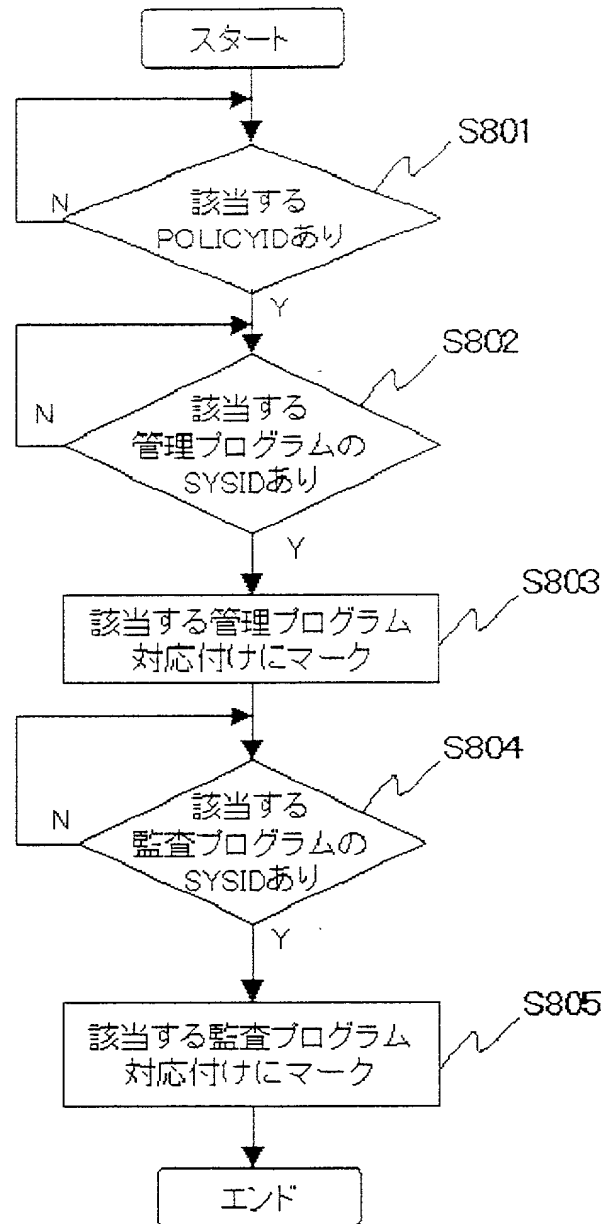
情報セキュリティポリシー選択画面

施策種別	識別と認証機能	▼	1001
セキュリティ施策	ネットワークにアクセス可能な端末の限定	▼	1002
	識別・認証情報用の良いパスワード 設定の実施		
使用可否	NO	▼	1003
	YES		

OK
閉じる

【図10】

図10



【図11】

図11

情報セキュリティポリシーの実施状況/
 セキュリティ施策の変更画面

1001

施策種別	識別と認証機能	▼
	アクセス制御機能 : 全て	
セキュリティ施策	ネットワークにアクセス可能な端末の限定	▼
	識別・認証情報用の良いパスワード設定の実施 : 全て	

1002

1101 1102

管理 監査 閉じる

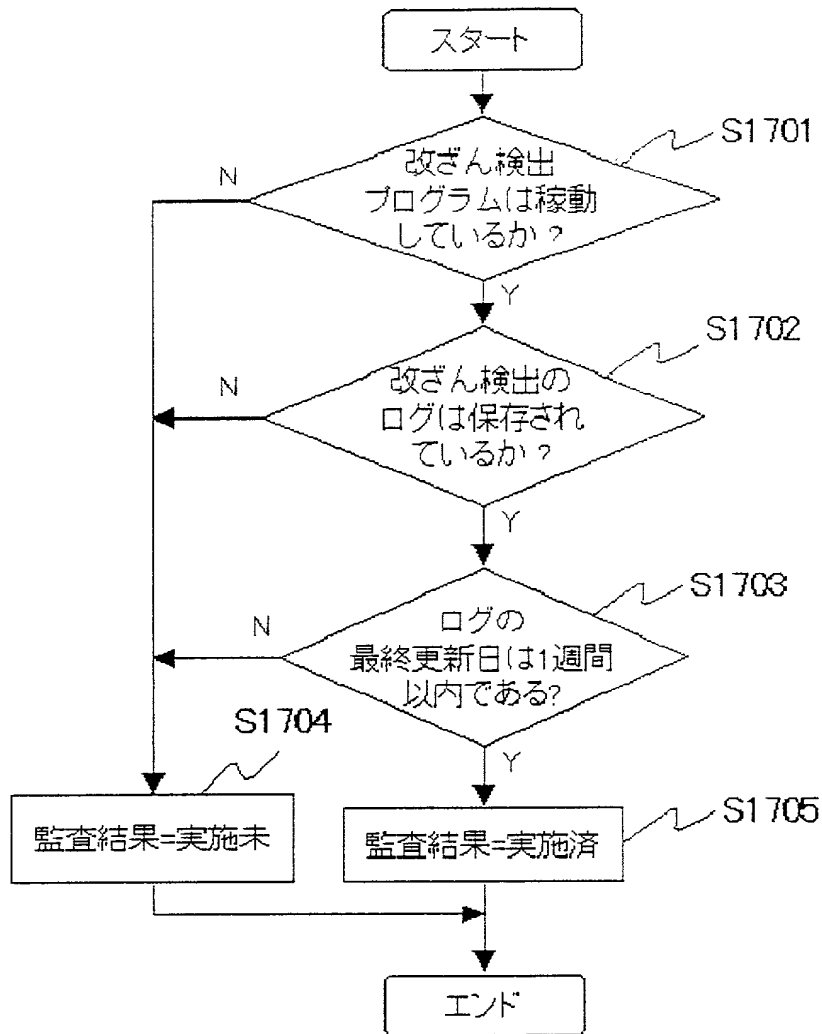
【図12】

図12

アカウント名	<input type="text"/>
パスワード	<input type="password"/>
パスワードに関するセキュリティ属性	
<input type="checkbox"/> パスワード長の長さが最低8文字以上であることを確認する。	
<input type="checkbox"/> パスワードが平易でないことを確認する。	

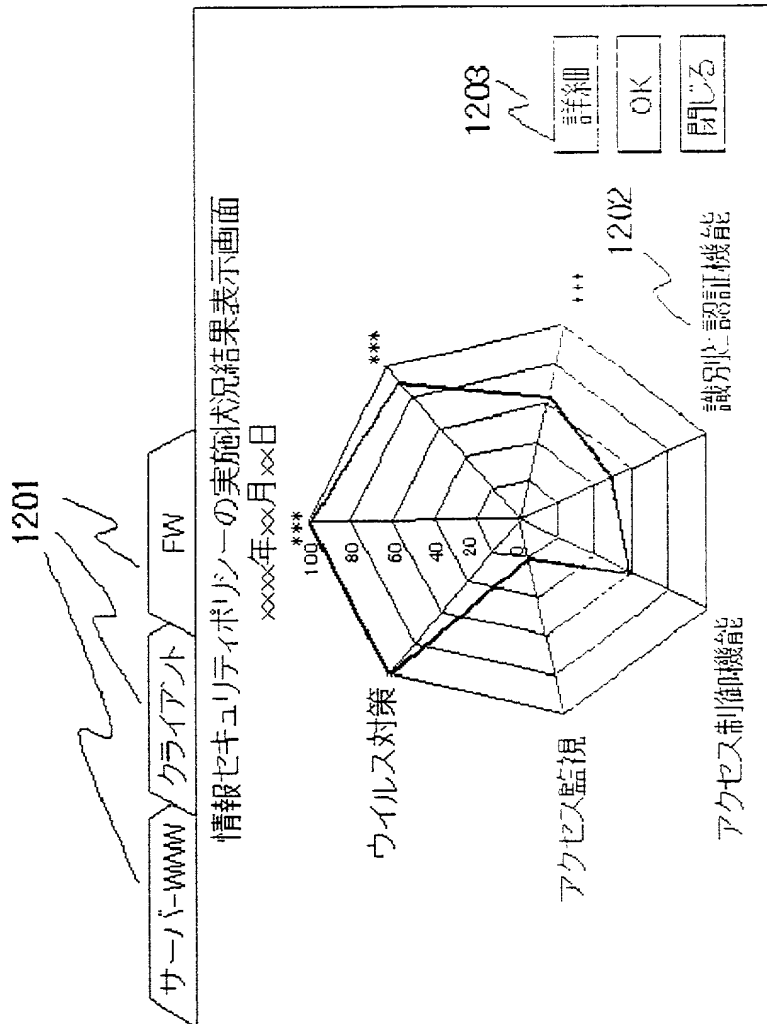
【図13】

図13



【図14】

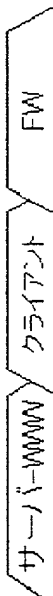
図14



【図15】

図15

1201



情報セキュリティポリシーの実施状況結果表示画面

xxxx年xx月xx日

1202

施策種別	割合(%)
入退室管理	100
ファイル管理	90
アクセス権限の設定・管理	64
識別と認証機能	50
アクセス制御機能	60
アクセス監視	20
ハッカー・ウイルス対策	100

1203

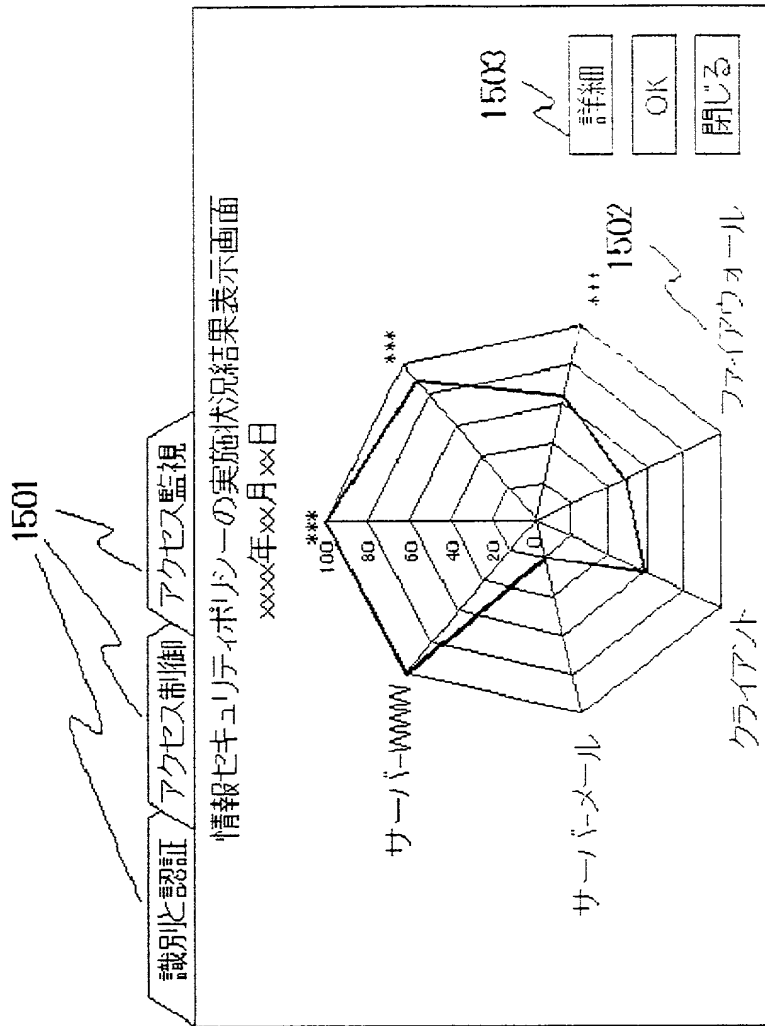
詳細

OK

閉じる

【図16】

図16



【図17】

図17

1401

識別と認証

アクセス制御

アクセス監視

情報セキュリティポリシーの実施状況結果表示画面
xxxx年xx月xx日

施策種別	セキュリティ施策	実施状況	選択
アクセス監視	データ・プログラムの改ざん検出の実施	実施済	✓
アクセス監視	ユーザ使用コマンドの記録	実施未	
アクセス監視	アクセスログの取得	実施未	✓
⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮

1403

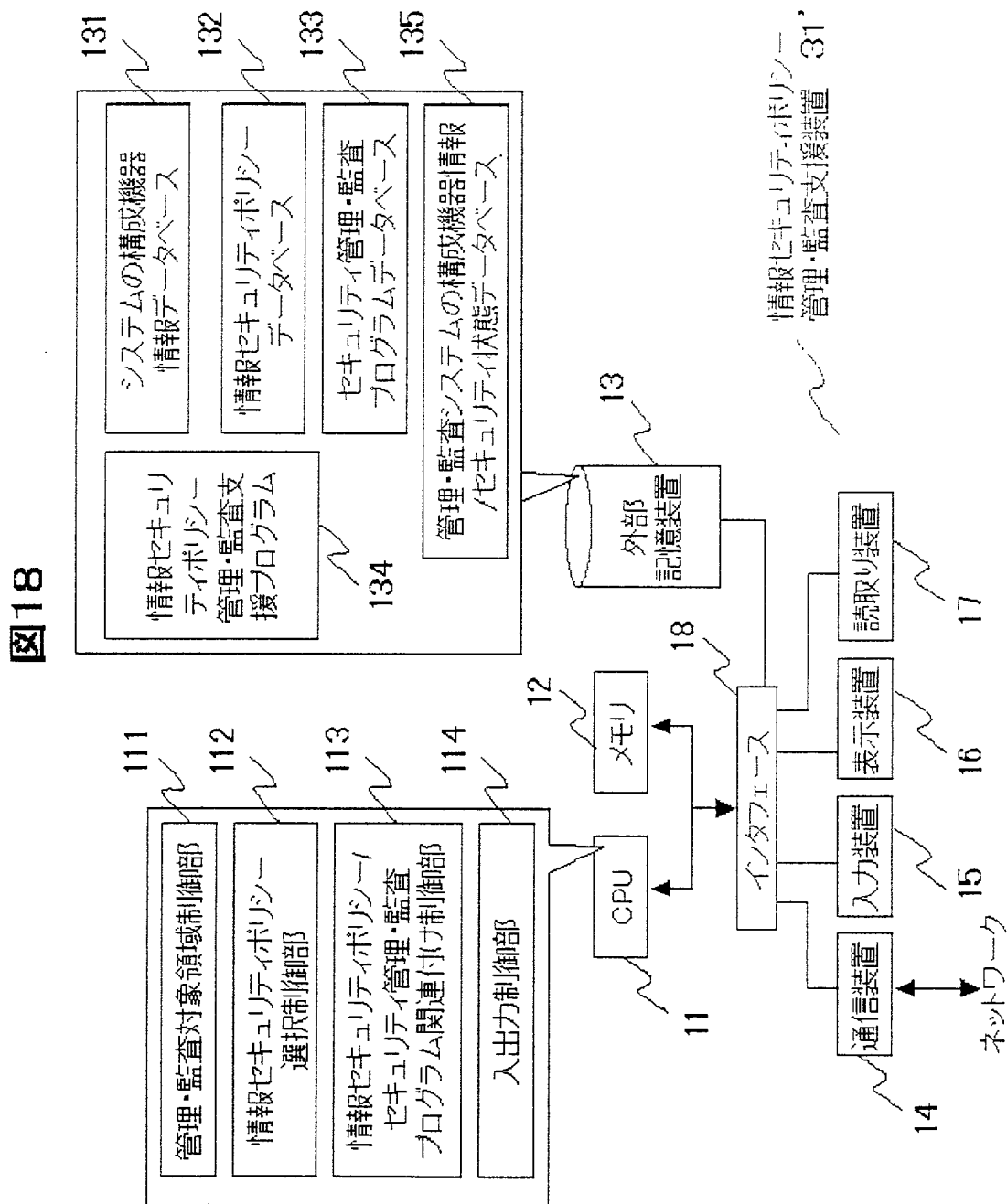
1404

管理

監査

閉じる

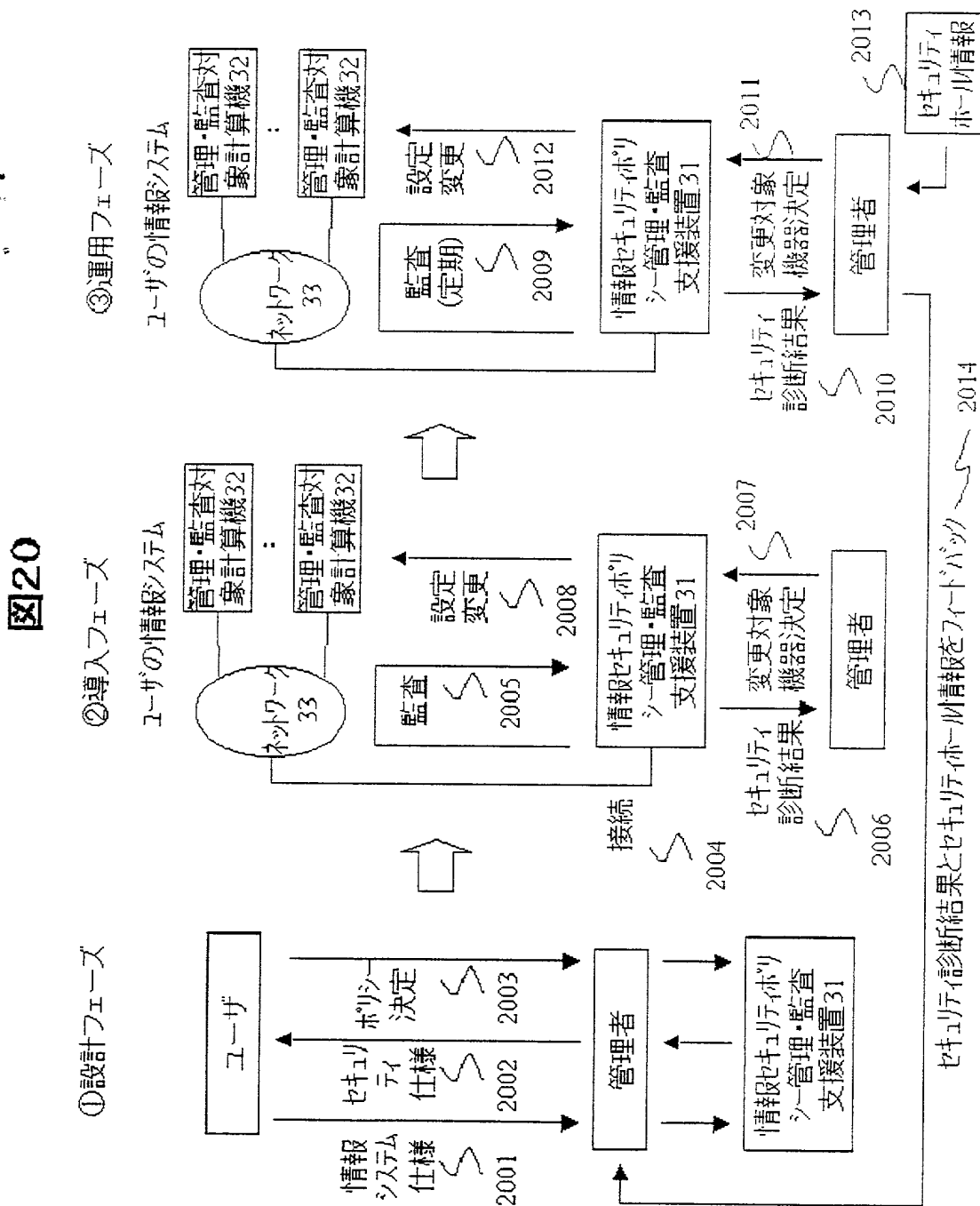
【図18】



61

[illegible]

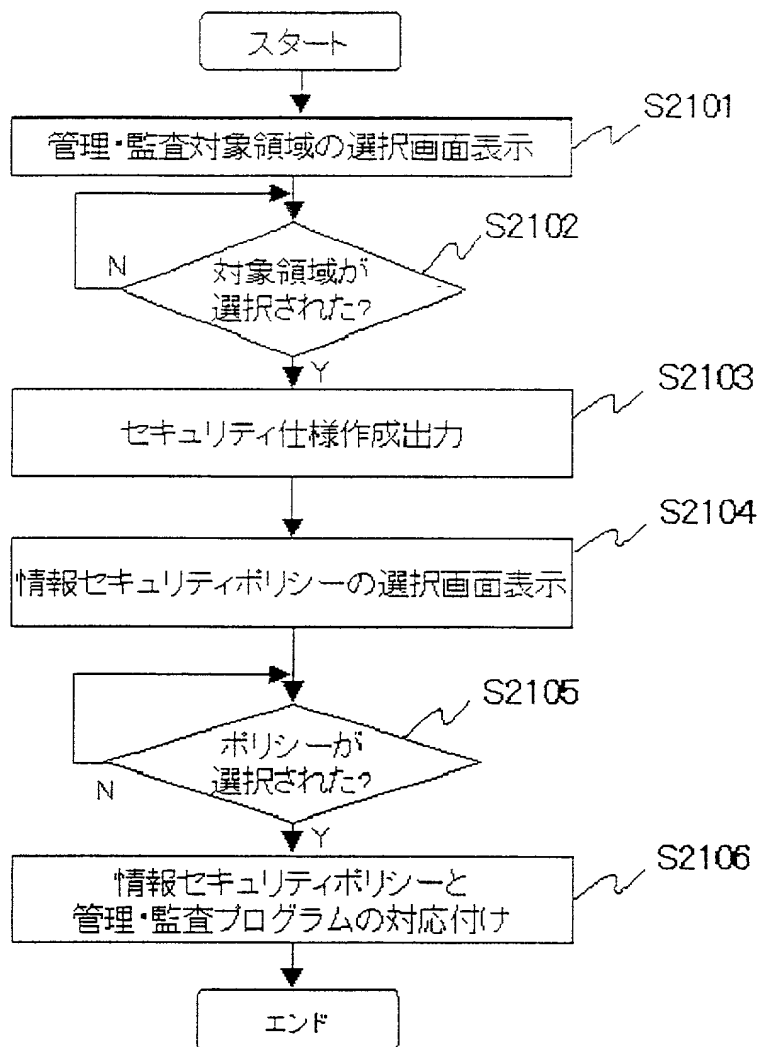
【図20】



【図21】

図21

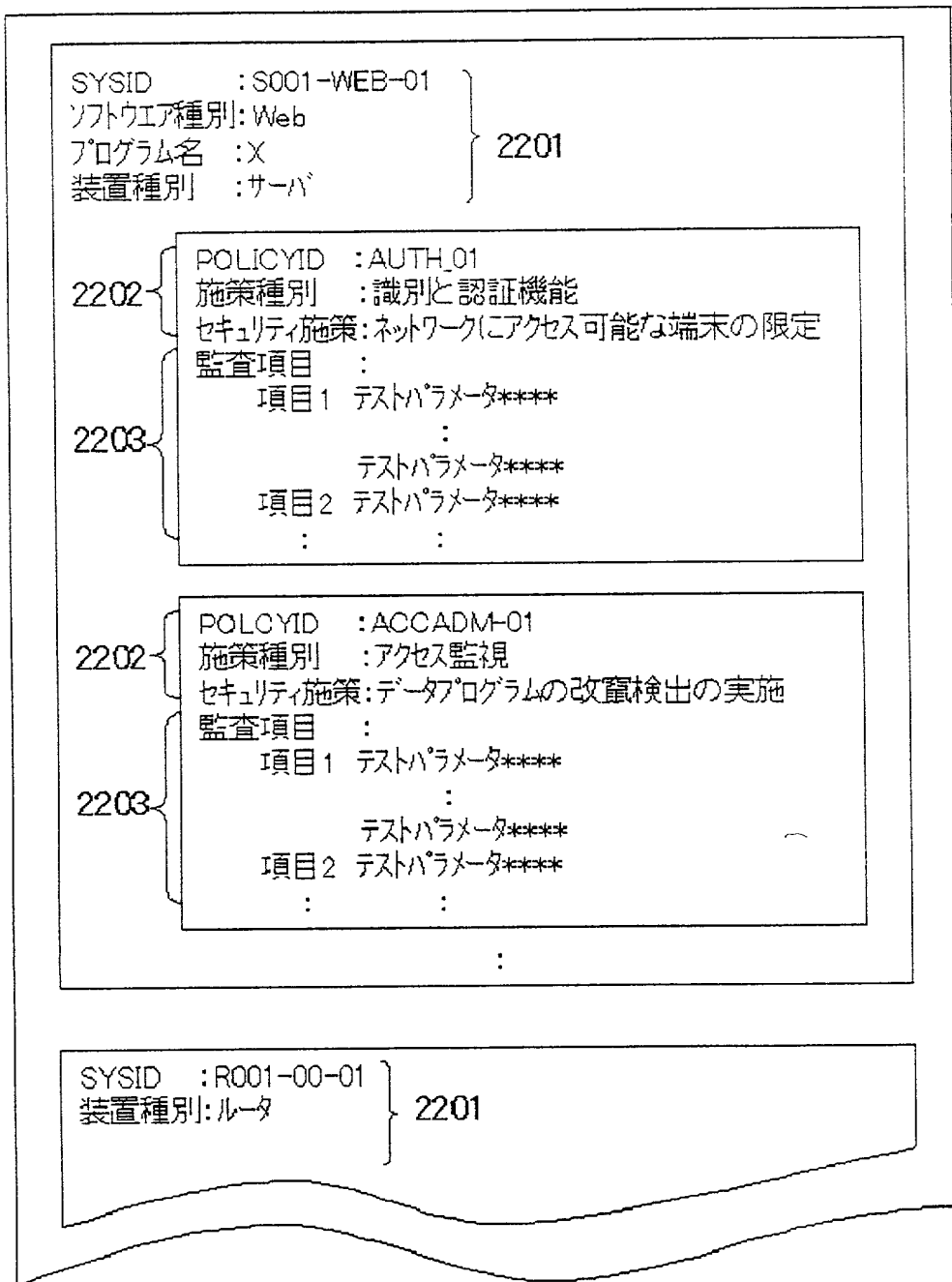
設計フェーズ



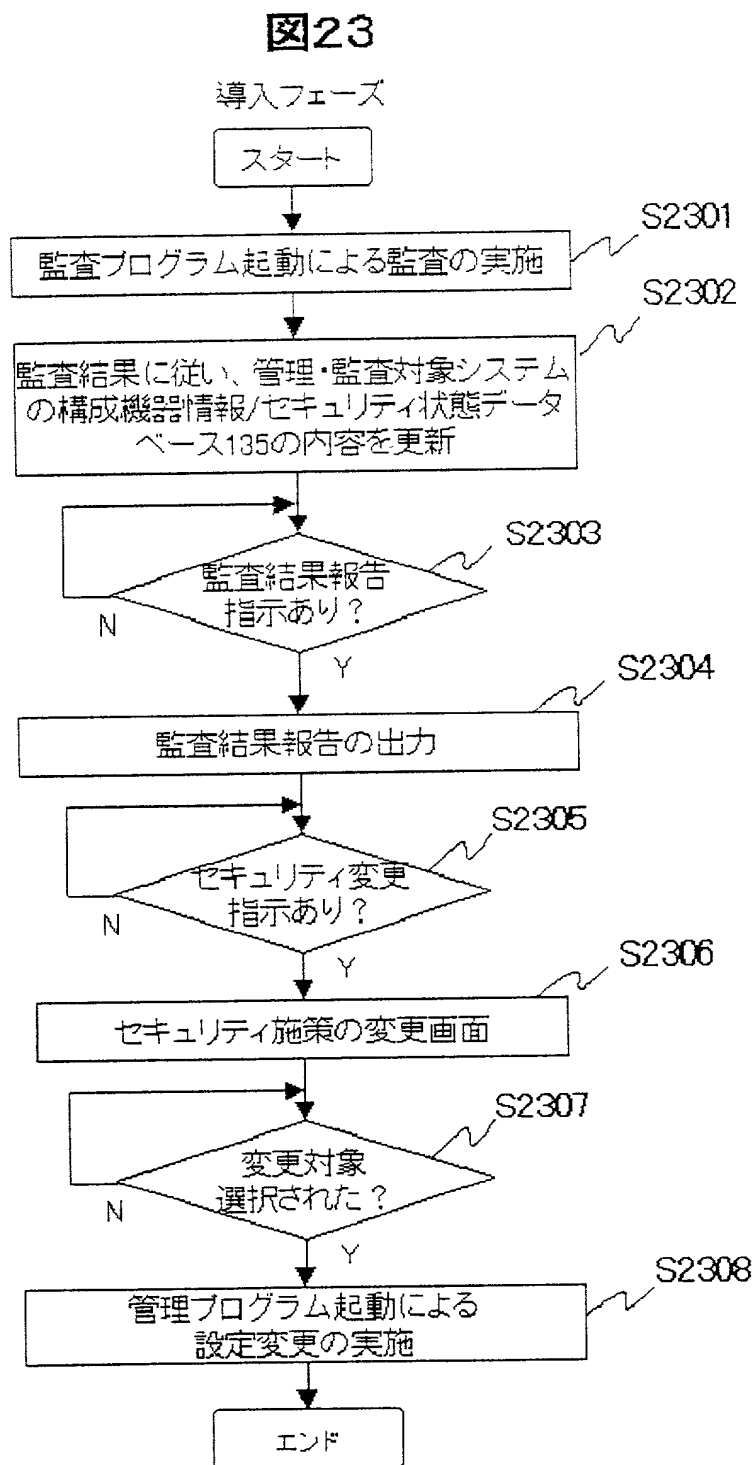
【図22】

図22

セキュリティ仕様書



【図23】



【図24】

図24

監査結果報告書

SYSID : S001-WEB-01		} 2401
ソフトウェア種別: Web		
プログラム名 : X	Ver/Patch: 1.0/-	
装置種別 : サーバ	装置型式 : ****	
2402	POLICYID : AUTH_01	
	施策種別 : 識別と認証機能	
	セキュリティ施策: ネットワークにアクセス可能な端末の限定	
	監査項目(施策実施の有無) : ○	
2403	項目1 テストパラメータ値****	
	:	
	テストパラメータ値****	
	項目2 テストパラメータ値****	
	:	
	:	
2402	POLICYID : ACCADM-01	
	施策種別 : アクセス監視	
	セキュリティ施策: データプログラムの改竄実施の検出	
	監査項目(施策実施の有無) : ×	
	項目1 テストパラメータ値****	
2403	:	
	テストパラメータ値****	
	項目2 テストパラメータ値****	
	:	
	:	
:		
SYSID : R001-00-01		
装置種別: ルータ		} 2401

TOP TO CH2360

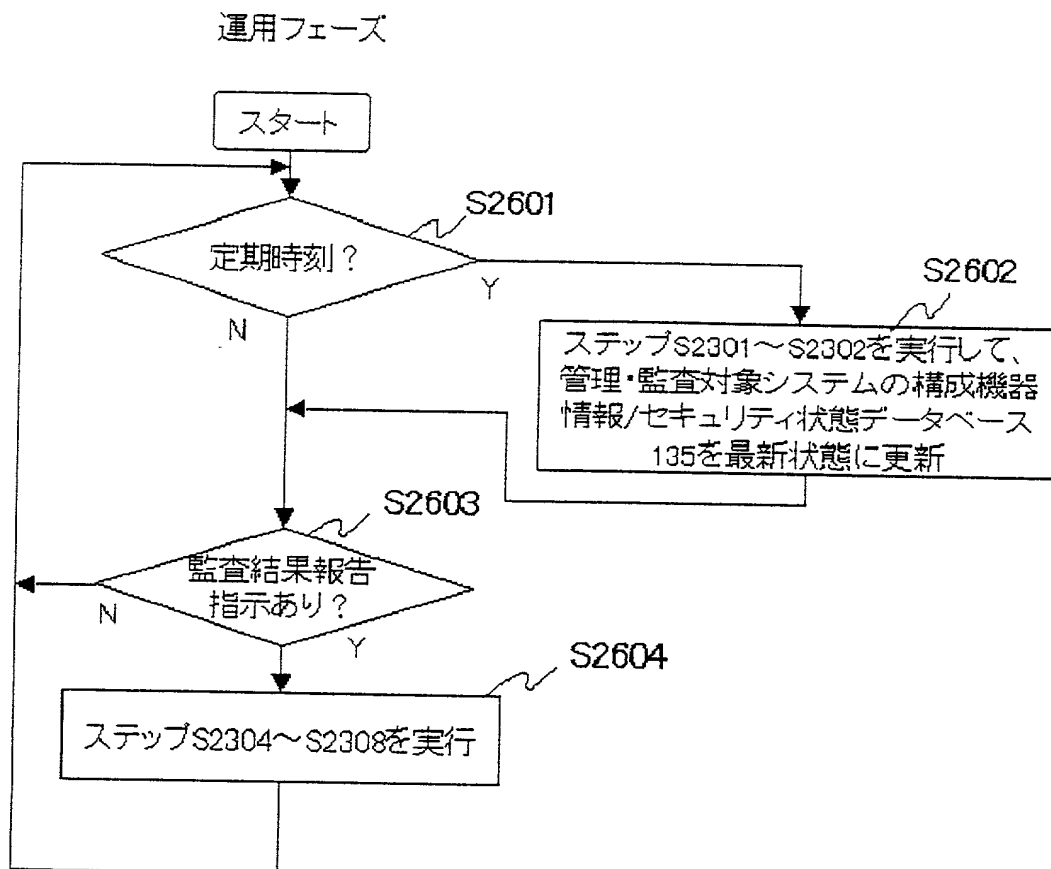
【図25】

図25

SYSID : R001-00-01		} 2401		
装置種別 : ルータ 装置型式 : ****				
POLICYID : ACCADM04		} 2402		
施策種別 : アクセス監視				
セキュリティ施策:不正アクセスの検知		} 2403		
監査項目(施策実施の有無) : ○				
時刻	アクセス種別	送信元アドレス	送信先アドレス	送信先ポート
00/05/15/12:00	SMTP	202.202.202.1	133.145.1.1	25/TCP
00/05/15/12:20	HTTP	202.213.111.6	133.145.1.6	80/TCP
00/05/15/12:32	SNMP	202.213.202.1	133.145.1.1	161/UDP
00/05/15/12:45	ICMP	202.213.111.6	133.145.1.1	-
00/05/15/12:47	FTP	202.202.202.1	133.145.1.1	21/TCP
:	:	:	:	:

【図26】

図26



TKS-2000-242360